Note

DNA PROFILES, COMPUTER SEARCHES, AND THE FOURTH AMENDMENT

CATHERINE W. KIMEL†

ABSTRACT

Pursuant to federal statutes and to laws in all fifty states, the United States government has assembled a database containing the DNA profiles of over eleven million citizens. Without judicial authorization, the government searches each of these profiles one-hundred thousand times every day, seeking to link database subjects to crimes they are not suspected of committing. Yet, courts and scholars that have addressed DNA databasing have focused their attention almost exclusively on the constitutionality of the government's seizure of the biological samples from which the profiles are generated. This Note fills a gap in the scholarship by examining the Fourth Amendment problems that arise when the government searches its vast DNA database. This Note argues that each attempt to match two DNA profiles constitutes a Fourth Amendment search because each attempted match infringes upon database subjects' expectations of privacy in their biological relationships and physical movements. The Note further argues that database searches are unreasonable as they are currently conducted, and it suggests an adaptation of computer-search procedures to remedy the constitutional deficiency.

INTRODUCTION

Having paid your debt to society, you are finally walking out the jailhouse door. And as you shake the prison dust off your feet, you resolve—successfully, as it turns out—never to commit another crime. No more frightening inmates. No more warden's ever-watchful eyes. You are free again, now and for the rest of your life.

---

† Duke University School of Law, J.D. expected 2013; University of North Carolina at Chapel Hill, B.A. in English Literature and Political Science, 2008. Thanks to my father, for his inspiration and example. Thanks also to the staff and editors on the *Duke Law Journal*, for their help, their work, and their friendship.

Or are you? Under the federal system and in every state, the government creates databases to store the DNA of every person convicted of a prescribed subset of offenses.[1] Law enforcement offices then search these databases one hundred thousand times a day, seeking, in the absence of any individualized suspicion, to bring unsolved crime after unsolved crime down upon database subjects' heads.[2]

This Note addresses the Fourth Amendment issues implicit in database searches of genetic profiles that are created after and because subjects were convicted of a statutorily designated crime. DNA-collection statutes have received a great deal of scholarly attention, but existing scholarship has focused almost exclusively on the initial extraction of DNA samples.[3] Moreover, scholars have assumed that if a sample's extraction is constitutional, then subsequent searches of its corresponding genetic profile must be constitutional as well.[4]

This Note is the first work squarely to question that assumption. It argues that comparisons of genetic profiles are Fourth Amendment searches because they reveal new information about subjects' biological relationships and their physical presence. Therefore, courts should require police to obtain a warrant before they compare two genetic profiles, just as police must obtain a warrant before searching

---

1. United States v. Kincade, 379 F.3d 813, 846–48 (9th Cir. 2004) (en banc) (Reinhardt, J., dissenting).

2. Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1391 (2008).

3. *See, e.g.*, Tracey Maclin, *Is Obtaining an Arrestee's DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (and Will) the Supreme Court Do*, 34 J.L. MED. & ETHICS 165, 178–81 (2006) (arguing that the "Louisiana and Virginia laws that authorize the taking of DNA samples from certain arrestees" are unconstitutional).

4. *See, e.g.*, Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 875 (2006) ("[O]nce the police lawfully collect DNA for one investigation, the Fourth Amendment permits reanalysis of that sample for a wholly separate investigation."); David H. Kaye, *DNA Database Trawls and the Definition of a Search in* Boroian v. Mueller, 97 VA. L. REV. IN BRIEF 41, 44–45 (2011), http://www.virginialawreview.org/inbrief/2011/08/04/kaye.pdf (defending the First Circuit's holding that the government is constitutionally permitted to "retrawl" the DNA profiles in its database "ad infinitum"); D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413, 424 ("[T]here is no 'search' when a lawfully acquired profile is entered in the database or is compared to the profiles from unsolved crimes."); Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 830–31 (2010) (claiming that database searches do not warrant the same "tenor of concern" as "physical confrontations, or even informational inquiries" and that a suspicion-based model is an ill-adapted means of regulating DNA-database searches).

a government-owned copy of a suspect's computer for evidence of a separate crime. This Note argues that procedures for searches of computers provide more than a ready model for DNA-database searches—rather, the DNA-database context actually justifies computer-search procedures better than computer searches do, and computer-search procedures would protect genetic privacy more effectively than they protect electronic privacy.

Part I introduces DNA, DNA databases, and the evolution of DNA-collection statutes. Part II provides a brief overview of Fourth Amendment doctrine. Part III draws upon that doctrine to argue that DNA-database searches are Fourth Amendment searches because the government violates weighty privacy expectations when it compares two genetic profiles. Finally, Part IV argues that the constitutional requirements of computer-search procedures highlight deficiencies in current DNA-database search procedures, and it questions whether society truly believes that electronic privacy is more important than genetic privacy—and thus whether current policies accurately reflect the country's social values.

I. BACKGROUND: DNA, CODIS, AND COLLECTION STATUTES

To understand the constitutional significance of DNA-database searching, it is important first to understand exactly what information is being searched in the databases and how this information comes into the government's possession. This Part will briefly explore DNA as genetic material and as evidence and then will explain the history and process of DNA-database construction.

A. DNA and DNA Profiling

Deoxyribonucleic acid (DNA) is present in most human cells.[5] DNA contains a sequence of genetic code that is three billion nucleotide base pairs long;[6] each sequence contains instructions for the production of the proteins essential to "the structure, function, and regulation" of every part of an individual's tissue and organs.[7] Thus, DNA constitutes predictive evidence of multitudinous aspects

5. Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J.L. & TECH. 309, 314 (2010).

6. *International Consortium Completes Human Genome Project*, NAT'L HUMAN GENOME RESEARCH INST. (Apr. 14, 2003), http://www.genome.gov/11006929.

7. *What Are Proteins and What Do They Do?*, U.S. NAT'L LIBRARY OF MED. (Nov. 5, 2012), http://ghr.nlm.nih.gov/handbook/howgeneswork/protein.

of an individual's mind and body, including the presence or future development of over four thousand heritable diseases.[8] Indeed, scientists now have decoded all three billion of the human genome's nucleotide base pairs[9] and have determined that "[m]any, if not most, diseases have their roots in our genes."[10]

The task of DNA profiling is to whittle this overwhelming quantity of genetic information down into one easily comparable profile. Profiling is possible because, although the vast majority of DNA is identical throughout humankind regardless of biological relationship, DNA does contain a relatively tiny number of variations, or polymorphisms, that render each individual's genetic material unique.[11] DNA profiling exploits these polymorphisms by creating a numeric record of the subject's genome at thirteen specified sites known to exhibit strong polymorphic tendencies and thought to be noncoding, meaning that those sites are unable to predict disease states or predispositions.[12] As a result, genetic profiles are easily differentiated.[13] The DNA-search process compares one numerically expressed DNA profile to another and assesses the similarities between the two.[14] Although the chances are infinitesimally small that two people who are not identical twins will exhibit the same polymorphisms at all thirteen loci,[15] the presence of some common variations indicates a biological relationship between two profiles' subjects. The more commonalities, the closer the likely biological connection.[16] A person can seek to match two profiles at all thirteen genetic markers—suggesting common identity between the

8. *Gene Mutations and Disease*, NAT'L CANCER INST. (Jan. 28, 2005), http://www.cancer.gov/cancertopics/understandingcancer/genetesting/page8.

9. *International Consortium Completes Human Genome Project*, *supra* note 6.

10. *Gene Mutations and Disease*, *supra* note 8.

11. Suter, *supra* note 5, at 314.

12. Boroian v. Mueller, 616 F.3d 60, 65–66 (1st Cir. 2010).

13. *See* Bruce S. Weir, *The Rarity of DNA Profiles*, 1 ANNALS APPLIED STAT. 358, 369 (2007) ("[T]he probability that a randomly chosen person has a particular forensic profile can easily reach the small value of 10^{-10}.").

14. Suter, *supra* note 5, at 319–20.

15. *See* Matthew Gilbert, *Police Seeing Double in Rape Case Involving Identical Twins*, CNN (June 7, 2004), http://articles.cnn.com/2004-06-07/justice/twins_1_identical-twins-dna-sample-dna-testing?_s=PM:LAW (recounting a Michigan rape investigation in which DNA was the only evidence and the DNA recovered from the scene was a complete match for two identical twins, both of whom had prior convictions for sex offenses).

16. Suter, *supra* note 5, at 318–19.

profiles' subjects—or one can seek to match profiles at only some of the genetic markers—suggesting the subjects' close kinship.[17]

Because DNA profiling and matching involve only thirteen purportedly noncoding loci, proponents have touted the process's respect for genetic privacy.[18] Even if the thirteen genomic markers from which genetic profiles are generated do not indicate health conditions, the information contained within a genetic profile still is sufficient to establish paternity[19] and kinship ties,[20] and to predict the subject's race, sex,[21] and even surname.[22] It also is important to remember that our understanding of the human genome is incomplete. Scientists continually discover medical value in genetic components once thought to be meaningless,[23] and it remains entirely possible that scientists one day will find that genetic profiles' composite loci code for important health determinants. Some evidence indicates that such a discovery is not unrealistic.[24]

B. DNA Databasing

The state's process for matching two DNA profiles begins with the creation of the profiles themselves, which the state then stores in searchable databases. The first step in the generation of this profile is to extract a biological sample from the subject, usually in the form of

17. *Id.* at 325–27. Some law enforcement offices have begun to search for "partial matches," or matches at less than all thirteen loci, which implicate the *relatives* of the matching profile's subject. *Id.* at 324. This practice of "familial searching" remains controversial and is not yet widespread in the United States. *Id.* at 325–27.

18. *See, e.g.*, H.R. REP. NO. 106-900, pt. 1, at 27 (2000) (stating that the thirteen loci "were purposely selected because they are not associated with any known physical or medical characteristics").

19. Joh, *supra* note 4, at 169.

20. Suter, *supra* note 5, at 318–19.

21. United States v. Kincade, 379 F.3d 813, 816 (9th Cir. 2004) (en banc).

22. Murphy, *supra* note 2, at 1331.

23. *See, e.g.,* Gina Kolata, *Study Discovers Road Map of DNA; A Key to Biology*, N.Y. TIMES, Sept. 6, 2012, at A1 (reporting on new studies showing that genetic material previously thought to be "junk" DNA in fact controls how genes function and contributes to the development of diseases like multiple sclerosis and lupus).

24. Suter, *supra* note 5, at 332 & n.155. This early evidence is, of course, contested. *See* David H. Kaye, Commentary, *Two Fallacies About DNA Data Banks for Law Enforcement*, 67 BROOK. L. REV. 179, 188 (2001) ("Contrary to the assertion in [Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127 (2001)], all [profile-composite loci] are noncoding, and none is known to correlate with any observable traits—stigmatizing or otherwise.").

blood or saliva.[25] The government then sends that sample to a state forensic laboratory, where state employees construct a genetic profile from the sample.[26] No federal statute governs the sample's disposition after the profile is created, and states—with the sole exception of Wisconsin—retain the tissue samples indefinitely.[27]

Once created, the genetic profile is uploaded into the Combined DNA Index System (CODIS),[28] a national database overseen by the Federal Bureau of Investigation (FBI)[29] and subdivided into local, state, and national levels.[30] The uploaded information includes the profile itself, a specimen identifier, and identification of the laboratory and technician who generated the profile.[31] Profiles enter CODIS at the local level and subsequently become accessible at the state and national levels.[32] As of September 2012, the national CODIS database contained more than 11,628,300 profiles, 11,176,400 of which were derived from voluntary donors and from categories of convicts, arrestees, and others whose DNA profiling is authorized or mandated by statute.[33] When police conduct a CODIS search, they compare a

25. *Kincade*, 379 F.3d at 816–17. Generally, the sample is taken while the subject is incarcerated or is otherwise subject to state control. *See, e.g.*, *Bureau of Forensic Services*, STATE OF CAL. DEP'T OF JUSTICE, http://ag.ca.gov/bfs/content/faq.php#dna (last visited Nov. 20, 2012). However, the government can (and has) taken biological samples for DNA profiling surreptitiously from unincarcerated individuals. Joh, *supra* note 4, at 860–62.

26. *E.g.*, CONN. GEN. STAT. ANN. § 54-102i (West 2009 & Supp. 2012). The profile-creation process takes twenty-three to thirty weeks. Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 732–33 (2007).

27. Suter, *supra* note 5, at 334 & n.172. Only eight state statutes explicitly proscribe testing for purposes beyond DNA profiling, and many statutes allow sample use for unspecified "law enforcement purposes." *Id.* at 335–36.

28. Maclin, *supra* note 3, at 166.

29. Suter, *supra* note 5, at 316.

30. Murphy, *supra* note 26, at 739.

31. Maclin, *supra* note 3, at 166.

32. *Id.* At all levels of stratification, CODIS profiles are divided into two categories: the "Forensic Index," which contains genetic profiles created from crime-scene samples and unidentified human remains, and the "Offender Index," which contains genetic profiles created from compelled samples and samples that were voluntarily contributed to assist an investigation (by relatives of missing persons, for example). Suter, *supra* note 5, at 315–16. For a discussion of the scope-of-consent issue surrounding the government's retention of genetic samples and profiles that were given voluntarily, see Kaye & Smith, *supra* note 4, at 423–30.

33. *CODIS—NDIS Statistics*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/codis/ndis-statistics (last updated September 2012).

profile generated from a crime-scene sample against each of the 11,176,400 profiles that constitute the national Offender Index.[34]

C. Evolving Authority for DNA Evidence Collection and Databasing

DNA evidence originally served only to support linkages between established suspects and specific crimes. Prosecutors first used DNA evidence in the late 1980s and early 1990s[35] to shore up cases against established suspects through proof that DNA evidence found at a crime scene matched the suspect's genetic profile.[36] During this period, the state could secure a DNA sample only with a court order based upon individualized suspicion, with the suspect's consent, or by investing the time needed to track the suspect and recover an "abandoned" DNA sample.[37]

Then, in the mid-1990s, Congress and state legislatures began to enact statutes that compelled submission of DNA samples from people who were not suspects in any investigation and that prescribed the creation of DNA databases.[38] The early DNA-collection statutes generally required a person to submit a biological sample upon conviction of a sex offense or a violent felony.[39] Since their enactment, however, DNA-collection statutes have expanded rapidly in scope. The statutes first were broadened to include people convicted of any felony.[40] Later, the statutes grew to encompass convicted misdemeanants.[41] The federal DNA-collection statute now authorizes the government to extract biological samples from illegal

34. *The FBI and DNA: Part 1: A Look at the Nationwide System That Helps Solve Crimes*, FED. BUREAU OF INVESTIGATION (Nov. 23, 2011), http://www.fbi.gov/news/stories/2011/november/dna_112311.

35. Murphy, *supra* note 26, at 731.

36. Suter, *supra* note 5, at 315.

37. John D. Biancamano, Note, *Arresting DNA: The Evolving Nature of DNA Collection Statutes and Their Fourth Amendment Justifications*, 70 OHIO ST. L.J. 619, 620 (2009).

38. Maclin, *supra* note 3, at 166.

39. Murphy, *supra* note 2, at 1329. As of 2008, all fifty states required DNA samples from people convicted of sex offenses and certain violent crimes. Kimberly A. Wah, Note, *A New Investigative Lead: Familial Searching as an Effective Crime-Fighting Tool*, 29 WHITTIER L. REV. 909, 926 (2008).

40. Murphy, *supra* note 2, at 1329. As of 2010, forty-nine states collected biological samples from all convicted felons. Idaho is the only state to resist this trend. *DNA Laws Database Topic Summaries*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/justice/dna-laws-database-topic-summaries.aspx (last visited Dec. 15, 2012).

41. Murphy, *supra* note 2, at 1329–30. As of 2006, thirty-eight or more states required biological samples from some subsection of misdemeanants. Rick Weiss, *Vast DNA Bank Pits Policing Vs. Privacy*, WASH. POST, June 3, 2006, at A1.

immigrants.[42] Finally, many states currently require biological samples from some or all arrestees,[43] from those acquitted by reason of insanity,[44] and even from juvenile offenders.[45] Meanwhile, CODIS has experienced a parallel expansion. The database was conceived as a pilot project among fourteen states in 1990, was formalized by federal legislation in 1994,[46] and was used by all fifty states by 1998.[47]

Rather than link identified suspects to specific crimes, the distinct purpose of DNA-collection statutes has been to facilitate the creation of genetic databases to assist law enforcement in generating suspects for unspecified past and future crimes.[48] So far, CODIS has resulted in "numerous" people being "convicted on the basis of a cold

42. 42 U.S.C. § 14135a(a)(1)(A) (2006 & Supp. IV 2011).

43. Murphy, *supra* note 2, at 1330. Because arrest rates are particularly high among young people, arrestee-collection statutes place many Americans under DNA surveillance for practically the entirety of their adult lives. *See* Erica Goode, *Many in U.S. Are Arrested by Age 23, Study Finds*, N.Y. TIMES, Dec. 19, 2011, at A16 ("By age 23, almost a third of Americans have been arrested for a crime . . . ."). Nearly half the states have enacted arrestee-collection statutes. *DNA Collection upon Arrest*, NAT'L CLEARINGHOUSE FOR SCI., TECH. & THE LAW AT STETSON UNIV. COLL. OF LAW (May 2011), http://www.ncstl.org/resources/DNACollection UponArrest. The federal courts so far have split on whether these statutes are constitutional. Corey Preston, Note, *Faulty Foundations*, 19 WM. & MARY BILL RTS. J. 475, 475–76 (2010). Most recently, a California state appellate court struck down the portion of California's DNA-collection law that required all felony arrestees to submit a DNA sample. People v. Buza, 129 Cal. Rptr. 3d 753, 755 (Ct. App. 2011).

44. *E.g.*, IOWA CODE ANN. § 81.2(3) (West 2009); N.J. STAT. ANN. § 53:1-20.20(g) (West 2009 & Supp. 2012). It is illustrative of the speed of collection statutes' expansion that Professor Erin Murphy was able to speculate as recently as 2008 that "[a]lthough no such statutes exist, it is not difficult to imagine the passage of legislation requiring the collection of DNA samples from mentally ill persons or other such individuals—not on the basis of being arrested or convicted of a crime, but rather as a result of simply being labeled 'dangerous.'" Murphy, *supra* note 2, at 1330.

45. Suter, *supra* note 5, at 317. As of 2006, thirty-one United States jurisdictions required DNA samples from some juvenile offenders. BUREAU OF JUSTICE STATISTICS, DNA FORENSICS: EXPANDING USES AND INFORMATION SHARING 2 (2006), *available at* http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=774.

46. Maclin, *supra* note 3, at 166; *see also* DNA Identification Act of 1994, Pub. L. No. 103-322, tit. XXI, subtit. C, 108 Stat. 2065, 2069 (codified as amended at 42 U.S.C. § 14132 (2006)) ("The Director of the Federal Bureau of Investigation may establish an index of . . . DNA identification records of persons convicted of crimes . . . .").

47. Maclin, *supra* note 3, at 166.

48. *See, e.g.*, *id.* at 167 ("[A] spokeswoman of Virginia Delegate Ryan McDougle, who sponsored [the bill] to expand the state's DNA database to cover arrestees, confirmed that the legislative intent behind the bill was to match the DNA of violent felony arrestees to DNA evidence from unsolved crimes and not to merely obtain the identity of those arrested by the state.").

hit alone."[49] As of January 16, 2009, law enforcement offices across the country benefited from over 79,000 cold hits that matched DNA profiles created from crime-scene samples to the profiles of CODIS subjects who had not been suspects in the investigations,[50] and the incidence of cold-hit matches continues to rise exponentially as CODIS acquires more and more DNA profiles.[51]

II. AN OVERVIEW OF BASIC FOURTH AMENDMENT DOCTRINE

The Supreme Court has stated that "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[52] The amendment was a resounding rejection of colonial America's experience with general warrants and writs of assistance, which had "permitted the King's officials to enter private homes and conduct dragnet searches for evidence of any crime."[53]

In keeping with the Fourth Amendment's purpose of protecting personal privacy, "some quantum of individualized suspicion is usually a prerequisite to a constitutional search or seizure."[54] Indeed,

---

49. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 296 (2010).

50. *Laboratory Services: Table 1: Statistics of Cold Hits and Success Rates Based on NDIS Data from CODIS*, FED. BUREAU OF INVESTIGATION (Jan. 16, 2009), http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2009/undermicroscope/table1.htm.

51. Murphy, *supra* note 26, at 740.

52. Schmerber v. California, 384 U.S. 757, 767 (1966); *see also* United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976) (finding that the purpose of the Fourth Amendment is to protect against "arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals"); Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891) ("No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law."). The Fourth Amendment itself reads,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

53. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005). *See generally* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 51–78 (1937) (describing the role that writs of assistance played in precipitating the American Revolution).

54. *Martinez-Fuerte*, 428 U.S. at 560; *see also* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 667 (1995) (O'Connor, J., dissenting) ("For most of our constitutional history, mass, suspicionless searches have been generally considered *per se* unreasonable . . . .").

the basic Fourth Amendment test for a "reasonable" search is the prior issuance of a judicial warrant based upon the state's proof of probable cause[55] to believe that the specific individual to be searched is or has been engaged in a specific criminal activity, specific evidence of which is likely to be found at the specific location listed in the warrant.[56] Warrants are the standard measure of reasonableness because the specificity that warrants require "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[57]

However, the warrant and probable-cause requirements underlying the reasonableness standard do not account for all searches sanctioned by the Fourth Amendment. The Supreme Court has carved out numerous exceptions to those requirements,[58] finely granulating when searches are reasonable without a warrant or probable cause in some fact patterns,[59] and at other times leaving

55. *See* United States v. Grubbs, 547 U.S. 90, 95 (2006) ("Probable cause exists when 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983))).

56. *See* United States v. Place, 462 U.S. 696, 701 (1983) (noting that a seizure is "*per se* unreasonable . . . unless it is accomplished pursuant to a judicial warrant issued upon probable cause").

57. Maryland v. Garrison, 480 U.S. 79, 84 (1987).

58. For example, special-needs searches are an exception to the warrant and individualized-suspicion requirements. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990). In other circumstances, no warrant is required, but there must be probable cause. *See* Arizona v. Hicks, 480 U.S. 321, 327 (1987) ("Dispensing with the need for a warrant is worlds apart from permitting a lesser standard of *cause* for the seizure than a warrant would require, *i. e.*, the standard of probable cause."). In still other situations, individualized suspicion is required, but at a lower level than probable cause, and the warrant requirement is dispensed with. *See Place*, 462 U.S. at 697–79 (holding that an officer's seizure of personal luggage on the basis of reasonable suspicion but without a warrant did not violate the Fourth Amendment); Terry v. Ohio, 392 U.S. 1, 27 (1968) (holding that an officer behaved constitutionally when he patted someone down on the basis of reasonable suspicion but with no warrant). Finally, sometimes the warrant requirement persists, but individualized suspicion is deemed unnecessary. *See* Camara v. Mun. Court, 387 U.S. 523, 540 (1967) (holding that municipal health inspectors constitutionally could conduct a suspicionless administrative search of an apartment, but that the tenant had the right to refuse them entry until they obtained a warrant).

59. *See, e.g.*, Bell v. Wolfish, 441 U.S. 520, 555–60 (1979) (holding that both prison-cell searches and visual body-cavity searches of pretrial detainees are reasonable under the Fourth Amendment); *Martinez-Fuerte*, 428 U.S. at 555–56 (stating that a vehicle search by roving border patrols "need not be justified by probable cause and may be undertaken if the stopping officer is 'aware of specific articulable facts, together with rational inferences from those facts, that reasonably warrant suspicion' that a vehicle contains illegal aliens" but prohibiting searches based simply on the vehicle's "general vicinity" to the border (quoting United States v. Brignoni-Ponce, 422 U.S. 873, 884 (1975))); United States v. Robinson, 414 U.S. 218, 235 (1973)

outcomes dependent upon an amorphous balancing test.[60] Still, this much has been established: a "search" occurs, and some measure of Fourth Amendment protection is triggered, when "the government violates a subjective expectation of privacy that society recognizes as reasonable."[61] Once a Fourth Amendment search has occurred, the only question is what degree of protection the Fourth Amendment will afford.[62]

III. ARE CODIS SEARCHES FOURTH AMENDMENT SEARCHES?

Naturally, then, the first question to arise in this Note's inquiry into constitutionality of CODIS searches is whether such searches are in fact "searches" within the meaning of the Fourth Amendment. To determine whether CODIS searches are independent Fourth Amendment searches, it is necessary to ask, first, whether those subject to the searches have a "subjective expectation of privacy" in the DNA profiles that the government lawfully has created and, second, whether society is prepared to recognize that expectation of privacy as "reasonable."[63] This Part will address each question in turn, ultimately arguing that subjects' continuing privacy interest in their genetic profiles is both actual and reasonable, and thus that the Fourth Amendment is implicated in every CODIS search.

A. Subjective Expectation of Privacy

CODIS searches meet the first prong of the Fourth Amendment test because CODIS subjects' actual expectation of privacy in their biological relationships and physical whereabouts persists even after the government has seized their DNA. First, the large volume and personal nature of the information in DNA gives rise to privacy expectations that are broader and more durable than the expectations surrounding other types of physical evidence. Second, CODIS

(holding that a search incident to a lawful custodial arrest is reasonable under the Fourth Amendment).

60. *See, e.g.*, Brown v. Texas, 443 U.S. 47, 50 (1978) ("The reasonableness of seizures that are less intrusive than a traditional arrest depends 'on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers.'" (quoting Pennsylvania v. Mimms, 434 U.S. 106, 109 (1977))).

61. Kyllo v. United States, 533 U.S. 27, 33 (2001).

62. *See Terry*, 392 U.S. at 19 (rejecting "the notions that the Fourth Amendment does not come into play at all as a limitation upon police conduct if the officers stop short of something called a 'technical arrest' or a 'full-blown search'").

63. *See Kyllo*, 533 U.S. at 33.

subjects have discrete privacy expectations in their genetic relationship with each person to whom their profile is compared and in their physical presence in each place where a forensic sample is found. Third and finally, under current jurisprudence, the government's continuous CODIS searches undermine CODIS subjects' subjective privacy interests in a profound and fundamental way.

Proponents of DNA-collection statutes contend that any invasion of subjects' privacy is complete upon the initial tissue extraction and the generation of the genetic profile, and that subsequent profile searches reexamine previously acquired information but reveal no "new, private or intimate information" and therefore create no new Fourth Amendment issue.[64] Because a "defendant could not possibly assert any expectation of privacy with respect to the scientific analysis of a lawfully seized item of tangible property, such as a gun," proponents argue, DNA likewise legitimately is "subject to a battery of scientific tests" once it is lawfully in the government's possession.[65]

This argument, however, overlooks the extreme qualitative difference between DNA and an "item of tangible property, such as a gun." Unlike an item of tangible property, DNA contains inherently personal information about an individual. Whereas a scientific analysis of a gun reveals only the properties of an inanimate and not particularly personal object, the significance of which is limited to the investigation at hand, the administration of "a battery of scientific tests" upon a person's DNA has the capacity to reveal the unique manner in which that person constitutes and regulates every aspect of her being.[66] The strict confidentiality attending the results of private genetic testing illuminates this intuitive understanding of privacy expectations in genetic information and contrasts strongly with

64. Boroian v. Mueller, 616 F.3d 60, 67 (1st Cir. 2010); *see also* State v. Hauge, 79 P.3d 131, 141–42 (Haw. 2003) ("[The defendant's] privacy interest in his blood and hair terminated at the time the sample was obtained pursuant to a lawful search and seizure."); People v. King, 663 N.Y.S.2d 610, 614 (App. Div. 1997) ("Privacy concerns are no longer relevant once the sample has already lawfully been removed from the body . . . ."); Kaye, *supra* note 4, at 45 ("Once the government lawfully acquires the [genetic] information, the marginal invasion of privacy that comes from using it later is minimal."). Even commentators who challenge the constitutionality of DNA-collection statutes tend to focus their attack on the initial extraction of genetic information rather than on subsequent database searches, or they simply assume that later database searches do not implicate the Fourth Amendment. *E.g.*, Joh, *supra* note 4, at 875.

65. *King*, 663 N.Y.S.2d at 614.

66. *See supra* notes 6–7 and accompanying text.

expectations regarding the results of a scientific manipulation of an ordinary item of property.[67] Finally, the prospect of the state's "battery" of tests is all the more threatening when one considers that the only limit that many DNA-collection statutes impose upon the state's use of biological samples is the vague restriction that the samples be used in fulfillment of "law enforcement purposes."[68]

Moreover, each attempt to match two genetic profiles does in fact reveal novel private information, in at least two ways. First, genetic matching uncovers what biological relationship exists between the persons whom the profiles identify.[69] Although one's genetic profile may be forever established in the initial profiling, genetic relationships are newly explored with each potential match, whether the government seeks a complete match or the more controversial partial match.[70] Therefore, because each profile comparison reveals new, otherwise-private information about the biological relationship between the profiles' subjects, subjective privacy expectations arise anew with each genetic comparison.

Importantly, these privacy expectations assert themselves regardless of the expected outcome of the genetic comparisons; it is

---

67. For example, it is the position of the World Health Organization that "[i]f anything, the confidentiality of genetic information may need to be guarded even more stringently than . . . ordinary [medical information]." *Genetic Testing*, GENOMIC RES. CTR., WORLD HEALTH ORG., http://www.who.int/genomics/elsi/gentesting/en (last visited Nov. 20, 2012); *see also* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (holding that a hospital program that informed police of pregnant patients who tested positive for cocaine use violated the Fourth Amendment, and viewing as important that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent").

68. Suter, *supra* note 5, at 335–36. For example, in writing about familial database searches, Professor Murphy worries that the disproportionately African-American and Hispanic CODIS population risks "open[ing] the door to a kind of twenty-first century racial eugenics in which crime and criminology are viewed largely as functions of genetics and biology." Murphy, *supra* note 49, at 321–25.

69. The concept that comparison can work a Fourth Amendment harm, even when one of the objects being compared is lawfully in the government's possession, is not new to the federal courts. *See* United States v. Concepcion, 942 F.2d 1170, 1173 (7th Cir. 1991) (finding that a Fourth Amendment search occurred when police inserted a key, lawfully in the state's possession, into a lock, without opening the door, in order to determine ownership of the key); United States v. Portillo-Reyes, 529 F.2d 844, 848 (9th Cir. 1975) (same). *But see* United States v. Lyons, 898 F.2d 210, 213 (1st Cir. 1990) (holding that no Fourth Amendment search occurred under a similar fact pattern); United States v. DeBardeleben, 740 F.2d 440, 445 (6th Cir. 1984) (same); Arizona v. Hicks, 480 U.S. 321, 324 (1987) (holding that an officer's copying down of a stereo's serial number to compare to a stolen stereo's serial number was not a Fourth Amendment search).

70. *See supra* text accompanying note 17.

not the case that people with "nothing to hide" are unalarmed by comparisons of their genetic material with someone else's.[71] Indeed, if people were concerned for their genetic privacy only when they believed that their genetic information was in some way inculpatory, then a man would not mind undergoing paternity testing not just for his (purported) children, but for the whole neighborhood. Similarly, a woman would not mind undergoing genetic screening not just with her spouse, but with all the men in town. The reality is that although genetic information is in itself intensely personal, comparisons between a person's own genetic makeup and someone else's acquire an *additional* layer of intimacy. In the same way that one's privacy is not less invaded because the paternity tests disclose that one is not a neighbor's parent, it is immaterial to the Fourth Amendment that CODIS searches most often reveal that two profiles are "not a match."[72] The Fourth Amendment "does not protect information per se," but instead "protects individuals against oppressive methods for acquiring that information."[73] It matters not that the majority of CODIS searches do not return a hit because the method of searching subjects' genetic profiles within a database for a match is "arbitrary and oppressive."[74]

---

71. This Note's argument is thus distinct from the straw man that proponents of DNA-collection statutes argue against, namely, that the Fourth Amendment should protect criminals' privacy interest in not being identified as the perpetrator of their crimes. *See, e.g.*, Kaye, *supra* note 4, at 46–47 ("[S]urely retrawls could reveal things a person would rather keep private. For example, an individual whose DNA profile is in the database . . . might well be concerned that later trawls will expose him as the perpetrator of an unsolved crime."). Justice Scalia offered a more ingenious articulation of the interplay between privacy and criminality, writing for the majority in *Arizona v. Hicks*, 480 U.S. 321 (1987): "there is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all," *id.* at 329.

72. *See* Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 362 (1998) ("[A] Fourth Amendment violation is 'fully accomplished' by the illegal search . . . ." (quoting United States v. Leon, 468 U.S. 897, 906 (1987))); *Hicks*, 480 U.S. at 325 (finding in the context of a search that consisted of moving a turntable a couple of inches that "[i]t matters not that the search uncovered nothing of any great personal value to respondent—serial numbers rather than (what might conceivably have been hidden behind or under the equipment) letters or photographs," because "[a] search is a search, even if it happens to disclose nothing but the bottom of a turntable"); *cf.* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home . . . *all* details are intimate details . . . .").

73. Kaye, *supra* note 4, at 47.

74. *See* United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976) ("The Fourth Amendment imposes limits on search-and-seizure powers in order to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.").

The second way in which CODIS searches expose information that would otherwise remain private is by divulging subjects' presence in noncriminal but embarrassing places. Wherever we go, we leave a trail of DNA behind us in the form of skin, saliva, hair, or blood.[75] Because modern DNA analysis requires only a tiny volume of tissue to generate a genetic profile, one leaves more than enough DNA behind to betray her presence in a space when she discards a spent cigarette or leaves her cup on the table after dining in a restaurant.[76] When the person shedding the DNA is a CODIS subject, then, the government can deduce her movements by collecting, profiling, and matching the DNA she continually leaves in her wake. The danger here is that CODIS subjects who were present in a place where a crime was committed—but at a time other than during its commission—would have their private movements exposed to scrutiny despite the lack of any independent connection between the CODIS subject and the crime.

Again, CODIS searches offend subjective expectations of privacy even in the absence of crime. After all, concern for privacy in one's physical movements is "not . . . solely the lot of the guilty. To be law abiding is not necessarily to be spotless," and "[u]nwanted attention from the local police need not be less discomforting simply because one's secrets are not the stuff of criminal prosecutions."[77] The government's practice of comparing all profiles within CODIS with every crime-scene sample that they generate has the capacity to reveal such intimate, noncriminal information as a CODIS subject's extramarital affair, the identity of her sexual partners, or her presence in a sex shop, strip club, or any number of other places rendered embarrassing by individual circumstance. CODIS searches' capacity to reveal personal, noncriminal activity in addition to criminal activity distinguishes the database searches from police practices that do not rise to the level of a Fourth Amendment search, such as canine sniffs that reveal only hidden contraband or blood tests that reveal only the presence of drugs in the suspect's system.[78]

---

75. Joh, *supra* note 4, at 858.

76. Jaxon Van Derbeken, *How Alleged Serial Killer Fell into Trap*, S.F. CHRON., Sept. 21, 2003, at A1. A DNA profile can be constructed from a microscopic six-cell biological sample. Murphy, *supra* note 26, at 733.

77. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 465 (1990) (Stevens, J., dissenting) (citation omitted).

78. *Compare* Illinois v. Caballes, 543 U.S. 405, 409–10 (2005) (stating that one of the critical factors rendering police use of a heat-sensing device unconstitutional in *Kyllo v. United*

Further, subjective privacy expectations are not extinguished by the subject's awareness that the government possesses his genetic profile. As a formal matter, courts repeatedly have held that one need not exclude others absolutely in order to maintain an expectation of privacy over a place or thing.[79] Given this framework, it makes sense to relax the exclusion requirement in the context of DNA because DNA is by its nature nonrivalrous and nonexcludable, yet highly personal.[80] In addition, practically speaking, if a person knows of no reason why she should be suspected of wrongdoing, she also expects that intimate aspects of her life—including her DNA—are free from state scrutiny. Therefore, just because a person knows that the police generated her DNA profile as a result of a prior conviction does not mean that that person expects her profile to be searched continually, for years, for unrelated crimes that she is not suspected of committing. Indeed, for evidence that individuals maintain an expectation of genetic privacy in the face of knowledge that police legitimately possess their DNA profile, one need look no further than the lawsuits brought by individuals who voluntarily gave DNA samples to assist with a specific investigation, only to find that the state retained their samples after the investigation ended and added their profiles to the government's files.[81]

States, 533 U.S. 27 (2001), was that "the device was capable of detecting lawful activity"), *with* United States v. Place, 462 U.S. 696, 707 (1983) (finding that "[a] 'canine sniff' by a well-trained narcotics detection dog" is not a Fourth Amendment search in part because "[i]t does not expose noncontraband items that otherwise would remain hidden from public view"), a*nd* Porter v. State, 93 S.W.3d 342, 346 (Tex. Ct. App. 2002) ("[A] government investigative technique, such as a dog sniff or chemical test, that discloses only the presence or absence of narcotics, and does not expose noncontraband items, activity, or information that would otherwise remain hidden from public view, does not intrude on a legitimate expectation of privacy and is thus not a 'search' for Fourth Amendment purposes.").

79. *See, e.g.*, Sara M. Smyth, *Searches of Computers and Computer Data at the United States Border: The Need for a New Framework Following* United States v. Arnold, 2009 U. ILL. J.L. TECH. & POL'Y 69, 97 ("The mere act of accessing a network does not, in itself, extinguish privacy expectations, nor does the fact that others may have occasional access to the computer."); *cf.* Katz v. United States, 389 U.S. 347, 359 (1967) (finding a subjective expectation of privacy in a closed public telephone booth made of glass).

80. *See* United States v. Kincade, 379 F.3d 813, 873 (9th Cir. 2004) (en banc) (Kozinski, J., dissenting) ("[W]e can't go anywhere or do much of anything without leaving a bread-crumb trail of identifying DNA matter.").

81. *See, e.g.*, John R. Ellement, *Keeping DNA Samples Limited, Court Rules*, BOS. GLOBE (Aug. 26, 2011), http://www.boston.com/news/local/massachusetts/articles/2011/08/26/keeping_dna_samples_limited_court_rules (recounting a six-year legal battle to recover a voluntary subject's DNA sample and profile).

Finally, for subjects who are aware of the government's continuous use of their genetic profile in CODIS, the government's database searches also injure subjective privacy expectations in a more latent, pervasive sense. The source of this pernicious harm is the fact that sustained suspicionless searches of DNA databases are "both visible (in that the subjects know they might be watched) and unverifiable (in that they do not know when they are being watched)."[82] Database searches are conducted *en masse* and without individualized suspicion, and subjects therefore cannot predict in what context their genetic code, and thereby their movements and relationships, will come under the government microscope. In this way, DNA-database searches can intrude upon subjects' "negative freedom," or their "freedom of not being interfered with."[83] The unpredictability of the searches can rob subjects of their generalized sense of privacy and compel them in all situations "to plan [their] actions while taking into account the public that has been forced on [them] and that judges those actions."[84]

The Supreme Court has recognized that negative freedom is an important aspect of citizens' privacy interests. For example, in *Lawrence v. Texas*,[85] the Court found that the preservation of negative freedom—or, as the Court called it, "transcendent" freedom—is fundamental to the sustenance of other aspects of liberty because "[l]iberty presumes an autonomy of self" and "spheres of our lives and existence . . . where the State [is not] a dominant presence."[86] Additionally, in *New York v. Ferber*,[87] the Court found indeterminate

82. Murphy, *supra* note 2, at 1385 (emphasis omitted).

83. *Id.* at 1386 (quoting ISAIAH BERLIN, *Two Concepts of Liberty*, *in* FOUR ESSAYS ON LIBERTY 118, 122–23 (1969)) (internal quotation marks omitted); *cf.* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("[T]he right to be let alone [is] the most comprehensive of rights and the right most valued by civilized men."), *overruled by Katz*, 389 U.S. 347, *and* Berger v. New York, 388 U.S. 41 (1967).

84. Emanuel Gross, *The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—The Proper Balance*, 37 CORNELL INT'L L.J. 27, 32 (2004). Some evidence suggests that people experience continuous or unfocused searches as more invasive than targeted searches related to specific investigations. *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 335 (2008) (documenting the results of an empirical study on perceptions of intrusiveness).

85. Lawrence v. Texas, 539 U.S. 558 (2003).

86. *Id.* at 562; *see also* Wolf v. Colorado, 338 U.S. 25, 27 (1949) ("The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society.").

87. New York v. Ferber, 458 U.S. 747 (1982).

surveillance of noncriminal acts to be a serious invasion of privacy interests.[88] Specifically, the *Ferber* Court found that child pornography injures the subject child's "interest in avoiding disclosure of personal matters" because the child "must go through life knowing that the recording [of her sexual act] is circulating," constantly "fear[ing] . . . exposure."[89] The child does not fear exposure as a criminal; the child is not a criminal. Rather, the child fears the deep humiliation that would attend the revelation of an intimate aspect of her person in a context that she cannot control—a personhood concern not wholly divorced from the privacy interest implicated in the content and physical presence of one's DNA.[90]

B. Reasonable Expectation of Privacy

CODIS searches meet the second prong of the test for a Fourth Amendment search because CODIS subjects' persistent expectations of privacy in their genetic relationships and physical movements are reasonable. First, society finds its own privacy expectations in these matters reasonable, and there is no constitutionally permissible reason to treat CODIS subjects' expectations any differently. Second, DNA's form and content distinguish DNA from evidence that is guarded by less robust privacy interests and align it instead with computer evidence, which the Fourth Amendment strongly protects.

Generally, Americans oppose the imposition of a national DNA database with universal coverage.[91] In defending the existing DNA-

88. *See id.* at 774 (holding that the right to free speech does not forbid states from banning the sale of material depicting children engaged in sexual activity).

89. *Id.* at 759 n.10 (quoting Whalen v. Roe, 429 U.S. 589, 599 (1977); David P. Shouvlin, *Preventing the Sexual Exploitation of Children: A Model Act*, 17 WAKE FOREST L. REV. 535, 545 (1981); and Ulrich C. Schoettle, *Child Exploitation: A Study of Child Pornography*, 19 J. AM. ACAD. CHILD PSYCHIATRY 289, 292 (1980)) (internal quotation mark omitted).

90. *See id.* ("[I]t is the fear of exposure and the tension of keeping the act secret that seem to have the most profound emotional repercussions." (citation omitted)).

91. *Cf., e.g.*, Simon A. Cole, *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*, *in* DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 63, 82 (David Lazer ed., 2004) ("Given the widespread popular view of DNA as 'genetic blueprint' and distrust of government, . . . politicians will be reluctant to support a universal genetic database. Thus, DNA databases can be expected to include everyone designated 'criminal' but not 'law-abiding' citizens."); Peter Neufeld, Panel Discussion at the Conference on DNA and the Criminal Justice System at Harvard University (Nov. 21, 2000) (transcript available at http://www.hks.harvard.edu/dna/transcribe_table_page.htm) ("[F]rankly . . . most people in the country are not in favor of the universal databank for a variety of reasons."). *Pineda v. Williams-Sonoma Stores, Inc.*, 246 P.3d 612 (Cal. 2011), is illustrative of Americans' overweening concern with privacy in their personal-identification

collection database, the government often finds it necessary to disavow the possibility of a universal database,[92] and police oppose their own inclusion in CODIS.[93] So, intuitively, it also should be true that society finds its own expectation of genetic privacy "reasonable," even its expectation of privacy in DNA profiles constructed from noncoding loci. Society believes that its privacy expectations are "reasonable" even though most people presumably do not plan to embark upon a crime spree.

But even if subjects' privacy interests are implicated by continuous database searches, defenders of the CODIS searches' constitutionality contend, the classes of people to whom DNA-collection statutes apply have a reduced expectation of privacy that database searches do not violate.[94] In other words, because the majority of those whose genetic profiles inhabit CODIS are present or former criminal convicts,[95] society is not prepared to recognize their genetic privacy interests as "reasonable," at least as far as their DNA profiles are concerned. Yet the Supreme Court has "repeatedly held" that prisoners do not forfeit their constitutional rights at the prison door, with the sole exception of rights that are "fundamentally inconsistent with imprisonment itself or incompatible with the objectives of incarceration."[96] Thus, in *Hudson v. Palmer*,[97] the Supreme Court found that a prisoner does not have a reasonable

---

information. In that case, a Williams-Sonoma customer brought a winning lawsuit to stop retailers from querying customers for their zip codes. *Id.* at 620.

92. *See, e.g.*, State v. Hauge, 79 P.3d 131, 143 (Haw. 2003) ("[T]he prosecution contends that [the defense's] concern that '[l]aw enforcement could gather a DNA databank of its citizens . . . appears to be an overstatement.'" (third and fourth alterations in original) (quoting the defense) (internal quotation marks omitted)).

93. *See* Dave Collins, *Police Wary of Giving DNA Samples*, ASSOCIATED PRESS, Oct. 16, 2001, *available at* http://www.huffingtonpost.com/2011/10/17/police-dna-samples_n_1015541.html ("Rank-and-file police from Connecticut to Chicago to Los Angeles have opposed what some experts say is a slowly emerging trend in the U.S. to collect officers' DNA. 'From a civil liberties standpoint, there are a lot of red flags,' said Connecticut Trooper Steven Rief, former president of the state police union.").

94. *See, e.g.*, Green v. Berge, 354 F.3d 675, 679 (7th Cir. 2004) (Easterbrook, J., concurring) ("[Prisoners'] privacy interests are extinguished by the judgments placing them in custody.").

95. Amitai Etzioni, *A Communitarian Approach: A Viewpoint on the Study of the Legal, Ethical and Policy Considerations Raised by DNA Tests and Databases*, 34 J.L. MED. & ETHICS 214, 216 (2006).

96. Hudson v. Palmer, 468 U.S. 517, 523 (1984); *see also* Kaye & Smith, *supra* note 4, at 418 ("The state could hardly provide that a citizen convicted of even the most heinous crime thereby forfeits the right to free speech, the privilege against self-incrimination, or the plethora of other rights secured by the Constitution.").

97. Hudson v. Palmer, 468 U.S. 517 (1984).

expectation of privacy in his prison cell because such an expectation "simply cannot be reconciled with . . . the needs and objectives of penal institutions,"[98] including the need to protect inmates, staff, and visitors from weapons that an inmate could conceal there.[99]

Griffin v. Wisconsin[100] is perhaps even more relevant to the issue of searching subjects' genetic profiles within a database because it involves the reasonable privacy expectations of individuals who have been convicted of a crime but who are not physically incarcerated.[101] In *Griffin*, a warrantless "special needs" search of a probationer's home was found constitutional, even though the search was justified by less than probable cause.[102] In deeming the search "reasonable" despite the lowered level of individualized suspicion, the Court held that probationers have a reduced expectation of privacy because their continued physical liberty depends upon their supervised compliance with conditions not applicable to generalized society.[103] This heightened supervision is in turn justified because "'the very assumption of the institution of probation' is that the probationer 'is more likely than the ordinary citizen to violate the law.'"[104] Because police must confirm probationers' adherence to probation restrictions even within the probationers' own homes, probationers enjoy only a reduced expectation of privacy inside their homes.[105]

In *Hudson* and *Griffin*, the Court recognized that convicts' reasonable expectations of privacy are reduced to the extent necessary for the imposition of the prescribed punishment as a practical matter. Yet neither *Hudson* nor *Griffin* held that convicts lose reasonable privacy expectations simply by virtue of being convicts. Indeed, the Court in *Hudson* was explicit that citizens do *not* lose their constitutional rights upon conviction of a crime.[106]

---

98. *Id.* at 526.

99. *Id.* at 526–27.

100. Griffin v. Wisconsin, 483 U.S. 868 (1987).

101. *Id.* at 870–72.

102. *Id.* at 872.

103. *Id.* at 874–75; *see also* United States v. Knights, 534 U.S. 112, 119 (2001) ("Inherent in the very nature of probation is that probationers 'do not enjoy the absolute liberty to which every citizen is entitled.'" (quoting *Griffin*, 483 U.S. at 874)); Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 365 (1998) ("Parole is a 'variation on imprisonment of convicted criminals.'" (quoting Morrissey v. Breyer, 408 U.S. 471, 477 (1972))).

104. *Knights*, 534 U.S. at 120 (quoting *Griffin*, 483 U.S. at 880).

105. *See Griffin*, 483 U.S. at 874 (defining and discussing the goals of probation).

106. *See* Hudson v. Palmer, 468 U.S. 517, 523 (1984) ("[W]e have insisted that prisoners be accorded those rights not fundamentally inconsistent with imprisonment."); *see also* Wolff v.

Under *Hudson* and *Griffin*, it is unclear from whence might stem the reduced privacy expectations of convicts subject to DNA-collection statutes. Unlike the searches at issue in those cases, searching the DNA profiles in CODIS cannot be necessary to enforce the punishments meted out to these convicts, as searching for evidence of a second crime clearly is unrelated to imposition of punishment for the crime for which the individual already has been convicted.[107] Furthermore, in stark contrast to probationers, once a DNA-database subject has paid her debt to society for a crime for which she has been convicted, the justice system positively is forbidden to "assum[e]" that she is "more likely than the ordinary citizen to violate the law."[108] Rather, if the former convict is ever again suspected of criminal activity, she will enjoy the benefit of "the undoubted law, axiomatic and elementary," which "lies at the foundation of the administration of our criminal law," that "there is a presumption of innocence" in her favor.[109] Finally, added to these essential problems is a temporal one. Prisoners complete their jail terms and probation periods end, and those individuals will regain normal privacy expectations—but the government retains and searches DNA profiles into perpetuity.[110]

Ultimately, one might concede that CODIS subjects have a continuing reasonable expectation of privacy in their DNA profiles but nevertheless argue that society simply would feel better knowing that former convicts were forever subject to genetic surveillance. However, this wish cannot overcome the Fourth Amendment's

---

McDonnell, 418 U.S. 539, 555–56 (1974) ("There is no iron curtain drawn between the Constitution and the prisons of this country.").

107. *See* Roe v. Marcotte, 193 F.3d 72, 81–82 (2d Cir. 1999) ("Clearly, the cases in which the Supreme Court has concluded that prisoners forfeit their Fourth Amendment rights upon incarceration deal with searches . . . for reasons of safety and orderly administration of prison facilities, concerns not implicated [by DNA-collection statutes].").

108. *Knights*, 534 U.S. at 120 (quoting *Griffin*, 483 U.S. at 880) (internal quotation marks omitted).

109. Coffin v. United States, 156 U.S. 432, 453 (1895).

110. *See* Johnson v. Quander, 440 F.3d 489, 498 (D.C. Cir. 2006) (holding that a felon who has completed probation does not have a right to purge his DNA sample even though he has completed his sentence). Thus, CODIS searches persist for longer than the law justifies other, more formalized methods of supervision. *Cf.* Murphy, *supra* note 2, at 1375 ("[T]he right story to tell about technological surveillance and control is not one of streamlining or one-for-one substitution, but rather one of proliferation, expansion, and enhancement. . . . [F]ocused on the strictures that govern what appears to be a more restrictive physical alternative, courts neglect to ask whether the more restrictive option would apply or, even if it did, whether any distinct burdens of the technological restraint demand some special procedural due process.").

protection of CODIS subjects any more than hospital administrators' desire to foster newborn health can supersede the Fourth Amendment's protection of new mothers who use crack cocaine.[111] Under current Fourth Amendment jurisprudence, laudable—or, at least, understandable—public policy goals do not supersede constitutional protection of individuals' privacy expectations.[112] And although historically a finding that a person is "dangerous" sometimes has been sufficient to warrant her incapacitation even in the absence of crime, such restraints generally are imposed only after painstaking individualized determinations[113] or when imposed in an extremely targeted fashion.[114]

A further argument against the reasonableness of subjects' continued expectation of privacy in their DNA profiles is that society does not "recognize an expectation of privacy in records made for

111. Ferguson v. City of Charleston, 532 U.S. 67, 85 (2001) ("[The respondents'] motive was benign rather than punitive. Such a motive, however, cannot justify a departure from Fourth Amendment protections . . . ."); *see also* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 459 (1990) (Brennan, J., dissenting) ("[C]onsensus that a particular law enforcement technique serves a laudable purpose has never been the touchstone of constitutional analysis."); Brown v. Texas, 443 U.S. 47, 52 (1979) ("The record suggests an understandable desire to assert a police presence [in the drug-ridden neighborhood]; however, that purpose does not negate Fourth Amendment guarantees.").

112. *Brown*, 443 U.S. at 52; *see also* Jason Tarricone, Note, *"An Ordinary Citizen Just Like Everyone Else": The Indefinite Retention of Former Offenders' DNA*, 2 STAN. J. C.R. & C.L. 209, 239 (2005) (noting that by the same logic used to justify indefinite, continuous searches of genetic profiles without individualized suspicion, "we could probably prevent most rapes (of women) . . . if we kept all men ages twelve to sixty-five interned in the desert, away from women and children").

113. *See, e.g.*, Kansas v. Hendricks, 521 U.S. 346, 358 (1997) (holding that nonpunitive civil commitment imposed after a prison term is constitutional because the applicable statute requires individualized findings of mental abnormality or personality disorder in addition to findings of dangerousness); Schall v. Martin, 467 U.S. 253, 279 (1984) (finding that family-court judges may predict a juvenile's future dangerousness based on "a host of variables," including the effectiveness of the juvenile's supervision at home, the juvenile's situation at school, and "any special circumstances that might be brought to [the judge's] attention by the probation officer, the child's attorney, or any parents, relatives, or other responsible persons accompanying the child"); Jurek v. Texas, 428 U.S. 262, 275–76 (1976) (holding that the statutory requirement that a prediction of the defendant's future dangerousness be considered in the jury's determination to impose the death penalty is constitutionally permissible because "the jury ha[s] before it all possible relevant information about the individual defendant whose fate it must determine"). *But see* Smith v. Doe, 538 U.S. 84, 103 (2003) (explaining that the state may make "reasonable categorical judgments that conviction of specified crimes should entail particular regulatory consequences," provided, however, that more debilitating constraints are implemented only upon individualized findings).

114. *See* Lewis v. United States, 445 U.S. 55, 67 (1980) ("Congress' judgment that a convicted felon . . . is among the class of persons who should be disabled from dealing in or possessing firearms because of potential dangerousness is rational.").

public purposes."[115] Some courts and commentators refer to this as the true-identity exception to Fourth Amendment protections.[116] The argument is that "DNA results are like fingerprints which are maintained on file by law enforcement authorities for use in further investigations."[117] Because police may reference existing fingerprint records in the FBI's national fingerprint database without implicating the Fourth Amendment, they, the argument goes, should also search the DNA database free of constitutional restraint.[118]

This argument is important because it has the potential to shift the debate toward either of two exceptions to the Fourth Amendment's warrant and probable cause requirements. If DNA databases have a record-keeping purpose, then arguably the process of extracting the samples, profiling them, and compiling the DNA database could be considered either an administrative search[119] or a special-needs search.[120] The question of whether the initial gathering of DNA samples constitutes an administrative or special-needs search is beyond the scope of this Note, which instead addresses CODIS searches occurring *after* the database has been assembled. Because these searches indisputably have an investigative purpose, they are ineligible for either exception.[121] The fingerprints-on-file analogy is

115. Smith v. State, 744 N.E.2d 437, 439 (Ind. 2001).

116. Kaye & Smith, *supra* note 4, at 430.

117. Bickley v. State, 489 S.E.2d 167, 170 (Ga. Ct. App. 1997) (quoting the trial court) (internal quotation mark omitted); *see also* Green v. Berge, 354 F.3d 675, 678 (7th Cir. 2003) ("[The purpose of the Wisconsin DNA law] is to obtain reliable proof of a felon's identity.").

118. *See* Johnson v. Quander, 440 F.3d 489, 499 (D.C. Cir. 2006) (rejecting petitioner's claim that the "Fourth Amendment applies to each 'search' of the [DNA] database"). Some courts even have suggested that subjects should thank their lucky stars for DNA surveillance because the only difference between fingerprinting and DNA profiling is that DNA is more accurate, and "the more accurate the identification method the less intrusive it is because of the associated reduced risk that the sample will result in misidentification." *See* United States v. Amerson, 483 F.3d 73, 86 (2d Cir. 2007). Of course, misidentification is not the privacy concern that CODIS searches present—rather, one of DNA matching's real privacy intrusions is its capacity definitively to identify a CODIS subject as having been present at a noncriminal, but embarrassing, situation.

119. Administrative searches must have a "subsidiary purpose" distinct from criminal-law purposes, but neither a concurrent criminal-law purpose nor the discovery of evidence of a crime in the course of an administrative search strips it of its administrative-exception status. New York v. Burger, 482 U.S. 691, 712, 716 (1987).

120. Special-needs searches' "primary purpose" is something other than "uncover[ing] evidence of ordinary criminal wrongdoing." City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000). For an examination of whether DNA-collection statutes authorize administrative or special-needs searches, see generally Maclin, *supra* note 3.

121. *See supra* notes 119–120.

relevant to whether a search of an existing database is a discrete Fourth Amendment search, however, and so a brief review of the issue is appropriate.

The principal argument against the DNA-as-fingerprint analogy mirrors this Note's first argument against the DNA-as-tangible-property analogy:[122] there is a gargantuan qualitative difference between DNA and fingerprints. Fingerprints are capable only of identifying their subjects.[123] In contrast, DNA has the capacity to identify subjects *and* to provide deeply personal information about biological relationships, behavioral predispositions, and disease states.[124] As Professor Elizabeth Joh has written, DNA is different because "[f]ingerprints do not promise [the] potential for yielding vast amounts of genetic information for government use, forever."[125] In this regard, and given the risk of governmental abuse of valuable personal information and the political vulnerability of the groups subject to DNA-collection statutes, it is small consolation that DNA-databasing statutes contain only a few meager safeguards against the government's misuse of information.[126]

The nature and form of DNA further bolsters one's reasonable expectation of privacy in the information contained in her genetic material, as opposed to on the surface of her fingertips. A person's DNA is hidden inside her body's tissue, encrypted in a code that scientists only comparatively recently began to crack.[127] Indeed, a person's genetic identity is so subtly expressed that one cannot know

122. *See supra* notes 66–68.

123. Joh, *supra* note 4, at 870.

124. *Id.* at 870–71.

125. *Id.* at 871.

126. *See* McDonald v. United States, 335 U.S. 451, 456 (1948) ("Power is a heady thing; and history shows that the police acting on their own cannot be trusted."); United States v. Kincade, 379 F.3d 813, 843 (9th Cir. 2004) (en banc) (Reinhardt, J., dissenting) ("Even governments with benign intentions have proven unable to regulate or use wisely vast stores of information they collect regarding their citizens."); SUSAN SONTAG, AIDS AND ITS METAPHORS 32–33 (1989) (explaining that "[t]he consequences of testing HIV-positive are even more punitive for those selected populations—there will be more—upon which the government has already made testing mandatory" and that these punitive consequences include the removal of personnel who test HIV-positive from "sensitive" military positions). The most basic safeguard built into the DNA-databasing process is that a subject's genetic profile includes only non coding loci. *See supra* note 18. The federal DNA-databasing statute and many state statutes also make it a crime to misuse a biological sample or DNA profile. *E.g.*, 42 U.S.C. § 14135e(c) (2006); CAL. PENAL CODE § 299.5(i)(1)(a) (West 2008 & Supp. 2012).

127. *See International Consortium Completes Human Genome Project*, *supra* note 6 (announcing that the Human Genome Project, an international effort to sequence the human DNA code, was completed in 2003).

the contents of her own DNA profile without the benefit of scientific testing. Obviously, then, the embedded, encrypted nature of a person's DNA differs dramatically from the familiar swirls that are visible on that same person's fingertips.

But perhaps a less obvious comparison is to encrypted information stored inside a computer. In the context of computers, courts have found that encryption and password protection create a reasonable expectation of privacy in the information thus encrypted or protected.[128] And although, unlike computer encryption, genetic coding is biological rather than volitional, that difference does not affect the expectation of privacy to which the coding gives rise. That scientists can decode the genome also does not defeat one's code-inspired expectation of privacy—after all, the government's computer scientists likewise can best most computer encryptions and passwords.[129]

IV. ARE CODIS SEARCHES "REASONABLE?" WARRANT AND INDIVIDUALIZED-SUSPICION REQUIREMENTS

Thus far, this Note has argued that each time law enforcement officers search a genetic profile in CODIS, they disrupt database subjects' subjective, reasonable expectation of privacy in her genetic information. Therefore, given that the Fourth Amendment is implicated afresh with each attempt to match a database subject's DNA profile with another DNA profile, the next issue to resolve is in what way the Fourth Amendment should guard subjects' reasonable expectations of privacy. The touchstone for this inquiry again is "reasonableness"; here, however, the Fourth Amendment is concerned with the reasonableness of the search—as opposed to the reasonableness of the subjects' privacy expectations.[130]

As has been mentioned, in crafting the standard of reasonableness that should apply to CODIS search procedures, there

128. Smyth, *supra* note 79, at 98; *see also, e.g.*, United States v. Buckner, 473 F.3d 551, 554 (4th Cir. 2007) (finding that password protection places the password-protected files within a "locked box" for Fourth Amendment purposes (quoting United States v. Block, 590 F.2d 535, 539 (4th Cir. 1978))).

129. *See The Year in Review*, FED. BUREAU OF INVESTIGATION (Dec. 29, 2011), http://www.fbi.gov/news/stories/2011/december/the-year-in-review-part-2/the-year-in-review-part-2 (collecting the FBI's 2011 cyber "takedowns").

130. Terry v. Ohio, 392 U.S. 1, 19 (1968) ("[T]he central inquiry under the Fourth Amendment . . . [is] the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security.").

is a diverse palette of options from which to choose.[131] In particular, much scholarly ink has been spilt on the applicability of the special-needs exception to the warrant and probable-cause requirements.[132] In these discussions, however, scholars have tended to focus their Fourth Amendment inquiries on the initial seizure of the tissue sample, ignoring or rejecting Fourth Amendment harms caused by the profile's later use.[133]

As a result of this focus, scholars almost entirely have neglected to consider the similarities between DNA evidence stored in government databases and computer evidence stored in government copies of hard drives lawfully seized by police.[134] Yet the parallels in nature, content, and privacy expectations between information stored in computers and in DNA make application of the rules governing computer searches an attractive solution to the problem of protecting the genetic information networked into CODIS's immense data-storage system. This Part begins by identifying similarities between DNA and computer evidence. It goes on to outline the increased protections that courts afford computers, as opposed to DNA, after government seizure. Next, this Part demonstrates the unconstitutionality of current CODIS search procedures by way of analogy to unconstitutional computer searches by general warrant. Finally, it argues that courts could best vindicate genetic privacy interests by requiring a modified version of computer-search procedures for each CODIS search.

---

131. *See supra* notes 54–60 and accompanying text.

132. *See, e.g.*, Kaye & Smith, *supra* note 4, at 434 (arguing that arrestee-collection statutes meet the special-needs test); Maclin, *supra* note 3, at 118 (arguing that sampling arrestees' DNA is not a valid special-needs search); Derek Regensburger, *DNA Databases and the Fourth Amendment: The Time Has Come To Reexamine the Special Needs Exception to the Warrant Requirement and the Primary Purpose Test*, 19 ALB. L.J. SCI. & TECH. 319, 386 (2009) (arguing that arrestee DNA-collection statutes should be analyzed under the special-needs rubric); Tarricone, *supra* note 112, at 248 (arguing that the special-needs exception does not apply to the retention of "an ex-felon's DNA sample and profile long after he has completed his sentence").

133. *See supra* note 4.

134. For a notable exception, see Kelly Lowenberg, *Applying the Fourth Amendment When DNA Collected for One Purpose Is Tested for Another*, 79 U. CIN. L. REV. 1289 (2011), which compares the treatment of government-seized biological samples to the treatment of government-seized computers, *id.* at 1312–13. This Note is indebted to Ms. Lowenberg's discussion of the similarities between computers and DNA. *See id.* at 1312 ("[B]oth [computers and DNA] store a large amount of intermingled information in a small space that cannot be parsed at the time of collection.").

A. Similarities Between DNA and Computer Evidence

DNA and computer evidence share at least three essential characteristics: both can have a near-dispositive effect on criminal investigations and prosecutions, both have an enormous storage capacity relative to their physical size, and both are repositories of intensely personal information.

First, computer and DNA evidence both are considered so persuasive that "in many cases" in which the state prevails, they are "the sole proof of guilt that exists."[135] Computer evidence can be the principal or only evidence forming the basis of a conviction either when the defendant is charged with perpetrating a common-law crime on a computer—fraud is a good example—or when the alleged offense is inherently computer-based.[136] Similarly, the existence of a genetic-profile match also can be outcome-determinative, as experience indicates that juries are willing to convict on the strength of DNA evidence alone,[137] and common sense suggests that defendants are more likely to plead guilty when DNA evidence can be marshaled against them.[138]

A second shared characteristic is the capacity to store an amount of information disproportionate to the physical size of the evidentiary medium.[139] Courts concur that "[c]omputers record and store a remarkable amount of information about what users write, see, hear,

---

135. *See* Murphy, *supra* note 26, at 743 (writing with regard to DNA evidence).

136. *See Online Privacy, Social Networking and Crime Victimization: Hearing Before the H. Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 111th Cong. 5–7 (2010) (statement of Gordon M. Snow, Assistant Director, Federal Bureau of Investigation) (discussing types of cybercrime). For example, crimes amenable to proof solely or principally by computer evidence include child-pornography and intellectual-property offenses. *See id.* at 25 (statement of Joe Sullivan, Chief Security Officer, Facebook, Inc.) (discussing the need for broader information access to better discover evidence of child pornography on social-networking websites); *id.* at 55 (statement of Joe Pasqua, Vice President for Research, Symantec, Inc.) (discussing the use of social-networking websites to obtain personal information on key corporate employees in an attempt to gain access to intellectual property).

137. Andrea Roth, *Safety in Numbers? Deciding When DNA Alone Is Enough To Convict*, 85 N.Y.U. L. REV. 1130, 1140–43 (2010); *see also* People v. Rush, 672 N.Y.S.2d 362, 363 (App. Div. 1998) (affirming a rape conviction when a DNA match implicated the defendant, although the only other evidence against him were photo and lineup identifications, and although the victim could not identify the defendant at trial).

138. *See* Roth, *supra* note 137, at 1143 n.55 (citing a defendant's entry of a guilty plea when the only basis for indictment was DNA evidence). *But cf.* Murphy, *supra* note 26, at 742 (noting that formal statistics on cases relying solely on genetic evidence are hard to come by).

139. Lowenberg, *supra* note 134, at 1310.

and do."[140] For example, the average one-hundred gigabyte home computer stores the equivalent of fifty million typed pages,[141] a veritable "library's worth of information."[142] Much of this storage capacity is devoted to personal information such as bills and finance, medical information (actual medical records, as well as the computer's memory of medical websites visited), personal correspondence, and records of other personal activities.[143] DNA stores a similarly large quantity of information. The DNA in even one drop of human blood contains all three billion of the human genome's nucleotide bases, all of which scientists have decoded.[144] The substance of this genetic information is extremely personal for reasons this Note has discussed already: DNA contains the instructions for the proteins that form and regulate our bodies.[145]

Third, and most problematic for Fourth Amendment purposes, both computers and DNA store information in a highly integrated manner, intermingling the data in such a way that any one item is difficult to extract from the system as a whole. In the case of computers, this means that files for which police have probable cause and a warrant to search, like records of drug sales, often are interspersed with unrelated personal files, like intimate emails.[146] The documents that justified the search also may be intermingled with

140. Kerr, *supra* note 53, at 532; *see also, e.g.*, United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008) ("[I]t is true that computers can store a large amount of material . . . .").

141. Kimberly Nakamaru, Note, *Mining for Manny: Electronic Search and Seizure in the Aftermath of* United States v. Comprehensive Drug Testing, 44 LOY. L.A. L. REV. 771, 781 (2011).

142. United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001). For the Tenth Circuit, this impressive capacity places computers beyond "the established categories of constitutional doctrine" and "[a]nalogies to other physical objects, such as dressers or file cabinets." *Id.*

143. *See* Kerr, *supra* note 53, at 543 (noting that this information includes, for example, the user's actions in frequently used programs, like word processors). Computers also record users' visits to pornographic websites, a digital foray indulged in by roughly one-fifth of all Internet users. Anton L. Janik, Jr., *Combating the Illicit Internet: Decisions by the Tenth Circuit To Apply Harsher Sentences and Lessened Search Requirements to Child Pornographers Using Computers*, 79 DENV. U. L. REV. 379, 379 (2001).

144. *International Consortium Completes Human Genome Project*, *supra* note 6.

145. *See supra* notes 7–10 and accompanying text.

146. *See* Kerr, *supra* note 53, at 543–47 (describing various methods by which a forensic examiner would seek to locate a particular file from among a computer's documentary and programmatic entanglement).

files evidencing unrelated and previously unsuspected criminal activity.[147]

The kind of information stored in DNA and the manner by which police access it create similar intermingling problems. In its descriptive capacity, DNA contains code that dictates tissue and organ development, but it also contains spans of nucleotide bases that only regulate (rather than create) bodily systems, as well as spans that appear not to code for anything at all.[148] The trick of DNA profiling, then, is to separate the purely identifying information from the genetic-coding information. The DNA-profiling process at least nominally solves this aspect of the intermingling problem by singling out and memorializing the nucleotide bases at only the thirteen specified noncoding loci.

However, a thornier intermingling problem arises with regard to DNA's capacity to communicate information about subjects' biological relationships and presence in physical spaces. The problem arises because the state first matches each forensic profile against all the other profiles in the state's possession and then, if there is no hit, the FBI matches it against every one of CODIS's over ten million offender profiles.[149] In neither case does the government make any effort to limit its search to individuals who law enforcement might reasonably believe to be relevant to the investigation.[150] The result is that police uncover an enormous amount of information about the genetic relationships between the source of the forensic sample and CODIS subjects, as well as information about CODIS subjects' presence in the place where the forensic profile was found. But even under the best-case, complete-match scenario, only a tiny fraction of that information is relevant to the government's investigation. Thus, just as computer data-storage systems intermingle information relevant to a criminal investigation with irrelevant personal information, so do police procedures for matching DNA profiles intermingle information relevant to their investigation—that is,

147. *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1270–71 (10th Cir. 1999) (noting that police found child pornography while searching the suspect's computer for evidence of drug sales).

148. *See The New Genetics: Chapter 1: How Genes Work*, NAT'L INST. OF GEN. MED. SCI., http://publications.nigms.nih.gov/thenewgenetics/chapter1.html#c1 (last updated June 9, 2011).

149. *The FBI and DNA Part 1: A Look at the Nationwide System That Helps Solve Crimes*, *supra* note 34.

150. *Cf. id.* (describing how a forensic profile is first compared to "all the offenders from [a] state's database," and then later may be compared to "all the 50 states' offender profiles").

profile matches wherein the CODIS subject is the perpetrator of the crime—with the irrelevant but personal information communicated by profile misses[151] and by profile matches wherein the CODIS subject is *not* the perpetrator of the crime.[152]

B. Differences in Current Treatment of Computer and DNA Searches

Despite their similarities in form and content, computer evidence and genetic profiles generally have received very different treatment under Fourth Amendment law.[153] Specifically, courts' protection of privacy interests in information stored on personal computers *even after* police lawfully have seized the machines stands in marked contrast to courts' denial of privacy interests in DNA profiles after individuals have been compelled to hand over a tissue sample.

Because the procedures governing the initial seizure of computers and DNA influence courts' subsequent treatment of the evidence, those procedures warrant a quick inspection here. Computer seizures must be authorized by a warrant and probable cause, per the basic Fourth Amendment standard.[154] Thus, in the course of a warranted search, police generally may seize computers that they believe contain evidence specified in their warrant.[155] Once a computer is in the government's possession, police create a perfect, read-only copy of the hard drive, including a copy of all the computer's files, programs, and metadata.[156] The government then searches its copy of the computer for the evidence enumerated in its search warrant.[157] In so searching, police are permitted to open every

151. For a discussion of privacy interests in information concerning biological relationships, see *supra* notes 69–74 and accompanying text.

152. For a discussion of privacy interests in information concerning physical movements, see *supra* notes 75–78 and accompanying text.

153. Some commentators have challenged this treatment. Noteworthy examples include Kelly Lowenberg, *supra* note 134, and Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 113 (2011). Josh Goldfoot is Senior Counsel of the Computer Crime and Intellectual Property Section of the Department of Justice and argues that computer searches should be stripped of their Fourth Amendment protections and, *inter alia*, be treated similarly to blood analysis. Goldfoot, *supra*, at 112 & n *, 113, 150–51.

154. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 3 (3d ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

155. United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008).

156. Kerr, *supra* note 53, at 540–41.

157. *Id.* at 540. Thus, like DNA searches, computer searches entail searching information that the government possesses "non-rivalrous[ly]" with the subject of the search. *Id.* at 560.

file on their copy of the computer, regardless of the file's apparent irrelevance to their investigation,[158] because "computer files can be disguised in any number of ingenious ways," and computer "data might be erased," "hidden," or even "booby trap[ped]."[159] However, courts restrict computer search *targets* to the documents and files specified in the search warrant.[160] As a consequence, searches intended to uncover evidence of all or different crimes are strictly off-limits.[161]

This restriction on computer-search targets has several important implications. First, even when a search warrant is based on a reasonable belief that a computer-centered crime, like possession of child pornography, has been committed, the warrant violates the Fourth Amendment by "provid[ing] the government with unrestrained access to electronic records of [the suspect's] daily activities and private affairs"[162] if it does not list the evidence for which the police plan to search the computer.[163] Instead of looking only for child pornography, courts fear, police "might review expense reports, income-related files and correspondence, and federal filing information in search of evidence of tax evasion," or "[o]fficers might read through e-mail correspondence in search of evidence of an internet-based phishing scheme."[164] Courts recognize that evidence of unsuspected crimes could well be found on the government's copy of a suspect's hard drive—and if the case law is any indication, child pornography often is found unexpectedly—but courts nonetheless have determined that a suspect's privacy interest in expense reports

158. *See* Manno v. Christie, No. 08-3254, 2008 WL 4058016, at *4 (D.N.J. Aug. 22, 2008) (noting that because an agent would have been authorized to briefly review all paper documents to determine their relevance to the warrant, it was similarly reasonable for an agent to open all computer files in search of relevant information); *cf.* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("[I]t is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.").

159. United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1168 (9th Cir. 2010) (per curiam).

160. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 154, at 90–91 ("If the agent comes across evidence of a crime that is not identified by the warrant, it may be safe practice to obtain a second warrant.").

161. United States v. Mann, 592 F.3d 779, 782–83 (7th Cir. 2010).

162. United States v. Rosa, 626 F.3d 56, 61 (2d Cir. 2010).

163. *Id.* at 62.

164. *Id.* at 61.

and emails outweighs the social value of prosecuting other discovered, but previously unsuspected, crimes.[165]

Second, courts' belief that warrants provide essential protection for digital information has influenced their development of additional procedural requirements for computer searches. For example, one court has eliminated the plain-view exception to the warrant requirement in the computer search context.[166] Additionally, some courts require government agents searching a computer to obtain a second warrant when, in the course of their original warranted search, they inadvertently come across evidence of a second crime.[167] Indeed, to "abandon" the first search to pursue evidence of the second crime is to violate the Fourth Amendment, and if the state falls prey to this temptation, it loses the right to use the evidence of the second crime in criminal proceedings.[168]

---

165. *See, e.g.*, United States v. Koch, 625 F.3d 470, 474–75 (8th Cir. 2010) (rejecting evidence of child pornography found by police in the course of a computer search for evidence of an illegal gambling operation); United States v. Highbarger, 380 Fed. App'x 127, 128 (3d Cir. 2010) (rejecting evidence of child pornography that police discovered while searching a computer for evidence of illegal drug dealing); *Mann*, 592 F.3d at 780–81, 786 (stating that a detective found child pornography while searching the defendant's computer for evidence of an unrelated crime and noting that "[a]lthough we now hold that [the detective's] actions were within the scope of the warrant, we emphasize that his failure to stop his search and request a separate warrant for child pornography is troubling"); United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (suppressing evidence of child pornography because the officer's computer search exceeded the scope of the warrant).

166. *See* United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1178 (9th Cir. 2010) (per curiam) (Kozinski, J., concurring) (repudiating the plain-view doctrine because it turns "all warrants for digital data into general warrants").

167. *Carey*, 172 F.3d at 1276; *see also* United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005) (stating that officers should hold irrelevant computer files until the new conditions and limitations of the search are established); People v. Carratu, 755 N.Y.S.2d 800, 807–09 (Sup. Ct. 2003) (relying on *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), to suppress images of false-identification documents discovered under a warrant for evidence related to another crime). U.S. Department of Justice guidelines note that it is good practice for agents to obtain a second warrant when they encounter evidence of a crime in plain view while conducting a computer search for evidence of a different crime. Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules To Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 340 n.148 (2010); COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 154, at 90.

168. *Compare Carey*, 172 F.3d at 1276 (finding a Fourth Amendment violation when a police officer abandoned his computer search for drug-related evidence to search for child pornography after coming across an image of child pornography in his original warranted search), *with* United States v. Burgess, 576 F.3d 1078, 1092–95 (10th Cir. 2009) (finding no Fourth Amendment violation when an officer obtained a second warrant after encountering one image of child pornography during his search of a computer for evidence of illegal drug activity).

In contrast to this type of individualized determination, DNA samples are seized from all members of statutorily defined groups,[169] regardless of the applicability of DNA evidence to the case that brought the subject within the collection statute's purview.[170] Thus, when a person meets the statutory requirements—for example, by being convicted of using a revoked credit card—the state seizes her DNA as a matter of course, without suspicion that the person is involved in any unresolved crime, and regardless of the fact that her conviction obviates any use for her DNA in connection with the crime with which she was charged.[171] So, although a suspect in a specific and unresolved crime maintains a privacy interest in the contents of a government-owned copy of her personal computer, lawful state seizure of a convict's biological sample terminates her Fourth Amendment rights with regard to the genetic profile generated from that sample. Once the DNA is in the state's hands, the police are free to examine its genetics, keep it in their database forever, and match it against any and all forensic DNA profiles, all without judicial authorization.[172]

What accounts for this difference? Part of the explanation may be that invasion of electronic privacy is a specter that judges fear

---

169. *See supra* notes 39–47 and accompanying text.

170. *See* Murphy, *supra* note 2, at 1331 (noting that no mandatory collection statute "requires any findings of particularized need for collection—the onetime felonious bad-check writer convicted forty years ago must provide a sample alongside the incorrigible rapist").

171. *See* ALA. CODE § 36-18-24(b)(1) (LexisNexis Supp. 2011) (mandating collection of a DNA sample from all convicted felons); *id.* § 13A-9-14(b)(2), (e) (LexisNexis 2005) (designating the use of a revoked credit card as a felony).

172. *See* Green v. Berge, 354 F.3d 675, 680 (7th Cir. 2004) (analogizing properly collected DNA to a fingerprint and noting that "the Fourth Amendment does not control how properly collected information is deployed"); State v. Hauge, 79 P.3d 131, 144 (Haw. 2003) (holding that once DNA is procured lawfully from a defendant, no privacy interest persists). *But see* Boroian v. Mueller, 616 F.3d 60, 68 (1st Cir. 2010) ("We do not hold . . . that once a DNA sample is lawfully extracted . . . , the individual necessarily loses a reasonable expectation of privacy with respect to *any* subsequent use of that profile."). Perversely, some courts find that categorical seizure in the absence of individualized suspicion bolsters the reasonableness of the seizures. *See* Nicholas v. Goord, 430 F.3d 652, 668–69 (2d Cir. 2005) (holding that the DNA-collection statute meets the special-needs test precisely because the DNA is collected apart from any investigation, and thus cannot further ordinary law enforcement purposes); Shelton v. Gudmanson, 934 F. Supp. 1048, 1051 (W.D. Wis. 1996) ("The standardized nature of the DNA collection process gives minimal discretion to the persons administering it . . . ."). *But cf.* Camara v. Mun. Court, 387 U.S. 523, 530–31 (1967) ("It is surely anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior. For instance, even the most law-abiding citizen has a very tangible interest in limiting the circumstances under which the sanctity of his home may be broken by official authority . . . .").

more than they fear DNA surveillance. Whereas judges have first-hand knowledge of their own embarrassing computer habits and electronically stored information, they likely have only a fuzzy understanding of comparably basic facts about their genomes. But additionally, the classes of people subject to DNA-collection statutes are distinctly "other" than most judges and lawmakers. DNA statutes often apply only to our justice system's collection of felons, violent offenders, and sex offenders,[173] groups who are disproportionately African-American and poor.[174] In contrast, suspects in computer crimes tend to be older, whiter, and wealthier than other categories of criminals.[175]

Another key distinction is the differing conceptual frameworks into which courts have fitted computers and DNA. On the one hand, a majority of courts understand a computer hard drive to be something akin to "a container that stores thousands of individual [sub]containers in the form of discrete files," each one of which is entitled to constitutional protection.[176] On the other hand, courts conceptually freeze DNA in its physical form, making it and its associated profile a unitary "item of tangible property, such as a gun"[177] that after seizure only "is examined, not 'searched.'"[178] The decision to view computers as containers of file-sized units of

173. *See, e.g.*, 42 U.S.C. § 14135a(a)(1)(B), (d) (2006) (requiring the director of the Bureau of Prisons to collect DNA from incarcerated felons, sex offenders, violent offenders, and offenders convicted of attempt or conspiracy to commit a felony, sex crime, or crime of violence).

174. Steven Raphael, *The Socioeconomic Status of Black Males: The Increasing Importance of Incarceration*, *in* PUBLIC POLICY AND THE INCOME DISTRIBUTION 319, 319 (Alan J. Auerbach, David Card & John M. Quigley eds., 2006); *see also* Kaye & Smith, *supra* note 4, at 452 ("[N]early 30% of black males, but less than 5% of white males . . . [are] imprisoned on a felony conviction at some point in their lives.").

175. *See* Goldfoot, *supra* note 153, at 161–62 (writing specifically with regard to child-pornography offenders). People arrested for such computer-intensive crimes as embezzlement and fraud also are largely white. *See Crime in the United States, Table 43: Arrests by Race, 2010*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/table-43 (last visited Nov. 20, 2012) (illustrating that in 2010, 66 percent of those convicted of fraud and 66.3 percent of those convicted of embezzlement were white).

176. Kerr, *supra* note 53, at 555; *see also* Walter v. United States, 447 U.S. 649, 654 (1980) ("Ever since 1878 . . . it has been settled that an officer's authority to possess a package is distinct from his authority to examine its contents."). *But see* United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (holding that one's privacy interests in her computer are compromised fatally when police view any of the computer's contents).

177. People v. King, 663 N.Y.S.2d 610, 614 (App. Div. 1997).

178. Goldfoot, *supra* note 153, at 113.

information, however, is a construction not mandated by the nature of the computer device. A computer just as tenably could be divided into units of folders rather than files,[179] or could be seen as a physical object that "does not contain things," but rather "is one thing:" one hard drive, which, once seized, may be examined freely.[180] Likewise, it also is possible to view DNA profiles as more informational than physical, and in terms of the relationships and presences they disclose, rather than the physical samples from which they are derived.

C. Unreasonableness of the Current CODIS Search Paradigm

Denying application of Fourth Amendment protections to CODIS searches by classifying DNA as a single, lawfully seized object misses the point of exactly how DNA-database searches violate reasonable privacy expectations. The greatest portion of the privacy invasion engendered by DNA surveillance comes not from the physical seizure and profiling of the sample, but from the repeated suspicionless CODIS searches that occur after the profile has been created.[181] Therefore, to the extent that the physical DNA specimen is extracted by standard medical procedures and is profiled according to thirteen noncoding loci, current search procedures are indeed "reasonable" in relation to the invasions involved in that initial search.[182] The real invasion of privacy arises when the subject's genetic profile is compared to other genetic profiles one-hundred thousand times a day, for the rest of the subject's life.[183] These

179. *See* United States v. Kim, 677 F. Supp. 2d 930, 949–50 (S.D. Tex. 2009) (conceptualizing a computer's component units in terms of folders).

180. Goldfoot, *supra* note 153, at 113.

181. *See supra* Part III.B.

182. *See, e.g.*, Johnson v. Quander, 440 F.3d 489, 496 (D.C. Cir. 2006) ("[T]he privacy invasion caused by a blood test is relatively small . . . . In *Schmerber* [*v. California*, 384 U.S. 757 (1966)], the Court upheld the warrantless extraction of a blood sample from a motorist suspected of driving while intoxicated, despite his refusal to consent to the intrusion. The Court noted that the intrusion occasioned by a blood test is minimal because such 'tests are a commonplace . . . and . . . for most people the procedure involves virtually no risk, trauma, or pain.'" (quoting *Schmerber*, 384 U.S. at 771)). This assumes the existence of adequate protections against government abuse of the sample and the profile, which is a contested proposition. *See supra* note 126 and accompanying text.

183. *See* Murphy, *supra* note 2, at 1390–91 (suggesting that the impairment of negative liberty inheres in surveillance as exemplified by the psychological effect of knowing that one's biometric profile is accessed repeatedly every day); *cf.* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451–53 (1990) (clarifying that the Court's holding that the sobriety checkpoint satisfied the special-needs test was limited to "the initial stop" and that "[d]etention of particular motorists for [a] more extensive" period "may require satisfaction of an individualized suspicion standard").

searches trample upon reasonable privacy expectations by tracking subjects' biological relationships and physical whereabouts forever, divorced from any degree of suspicion that the subject engaged in any of the criminal activities in connection to which her profile is searched. It is in relation to these searches that current search procedures are wholly unreasonable.

Formally, CODIS searches are presumptively unreasonable because they are searches conducted in the absence of a warrant.[184] However, as Professor Eve Primus has written, "[f]or some time, . . . experts have understood that warrantless searches are in practice common" and that "[a]s long as the government is reasonably pursuing a legitimate government interest, the warrant and probable cause requirements regularly fade away."[185] For this reason, CODIS searches' similarities to constitutionally impermissible computer searches by general warrant are particularly helpful in highlighting the unreasonableness of the CODIS search paradigm.

CODIS searches are, in essence, general-warrant computer searches turned on their head: instead of searching a single computer for evidence of any and every crime, DNA matching searches any and every CODIS subject for evidence of one particular crime (times one hundred thousand, every day).[186] So, inasmuch as a computer search for evidence of any crime is an impermissible exploratory search,[187] and inasmuch as courts refuse the government's request to "take [all of a suspect's computer equipment] back to the lab, have a good look around and see what we might stumble upon,"[188] courts also should

184. United States v. Jacobsen, 466 U.S. 109, 114 (1984).

185. Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 255 (2011); *see also supra* notes 58–60 and accompanying text.

186. Murphy, *supra* note 2, at 1391.

187. United States v. Rosa, 626 F.3d 56, 61 (2d Cir. 2010).

188. United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1171 (9th Cir. 2010) (per curiam). This case is a wonderful example of courts' comparatively favorable privacy treatment of electronic evidence because its facts evoke medical-privacy concerns but also involve electronic recordkeeping. In that case, the Ninth Circuit found that federal agents violated the Fourth Amendment when they seized and examined hundreds of baseball players' steroid blood-test results because the agents had probable cause to examine only ten players' records. *Id.* at 1170–72. The same court that upheld a suspicionless DNA-seizure statute, *United States v. Kincade*, 379 F.3d 813, 835 (9th Cir. 2004) (en banc), then ordered the government to return the unsuspected players' test results in order to restore their privacy interests, which had been intolerably impaired by the seizure, *Comprehensive Drug Testing*, 621 F.3d at 1173. The outcome offers a particularly interesting parallel to issues of DNA-database searches, given that one might imagine that professional baseball players as a class are more likely than the general population to engage in illegal steroid use, just as once-incarcerated criminals as a class are

question a protocol that allows government agents to engage in fishing expeditions to connect DNA-database subjects with all and sundry crimes, none of which they actually suspect any of the subjects of committing.[189]

D. Modifying Computer-Search Procedures for Application to DNA-Database Searches

By virtue of their continuing respect for owners' privacy following computer seizures, courts' treatment of computer searches offers an attractive solution to DNA-database searches' problematic intermingling of relevant and irrelevant personal information. Moreover, computer and DNA-database searches threaten the same type of governmental abuse, making the same type of procedural protections appropriate. With computer searches, the danger is that police will go after a suspect for every crime for which they can find a scrap of evidence on the computer, regardless of the contours of their original suspicion.[190] DNA-database searches amount to the same thing because CODIS searches are most realistically seen not as one-off searches for the perpetrator of a single crime, but as a continuous stream of searches in which investigators hound CODIS subjects for every crime for which they have one scrap of evidence (a DNA sample) to compare.

However, to account for the different logistical issues that arise in computer and DNA searches, some modifications should be made to the computer-search model before it is applied to genetic-profile searches. Specifically, courts should continue to allow initial suspicionless seizures of biological samples but should require a warrant and probable cause for later searches of the DNA profiles

---

more likely than the general population to commit a future offense. *See Mitchell Report: Baseball Slow To React to Players' Steroid Use*, ESPN.COM (Dec. 14, 2007, 11:29 AM ET), http://sports.espn.go.com/mlb/news/story?id=3153509 ("Doping was widespread by stars as well as scrubs, the report said . . . ."); Eric Holder, *Second Chances and Safer Communities*, JUSTICE BLOG (May 24, 2012), http://blogs.justice.gov/main/archives/2212 ("[R]oughly 40 percent of those released return to prison or jail within three years.").

189. *See* Stanley v. Georgia, 394 U.S. 557, 571–72 (1969) (Stewart, J., concurring in the result) (explaining "that 'exploratory searches . . . cannot be undertaken by officers with or without a warrant'" is a "basic constitutional rule" (quoting United States v. Rabinowitz, 339 U.S. 56, 62 (1950))); *cf.* Camara v. Mun. Court, 387 U.S. 523, 535 (1967) ("[I]n a criminal investigation, the police may undertake to recover specific stolen or contraband goods. But that public interest could hardly justify a sweeping search of an entire city conducted in the hope that these goods might be found.").

190. Or, in Professor Murphy's formulation, the danger of the "overzealous, overstepping constable." Murphy, *supra* note 4, at 830.

generated from those samples, and the biological samples themselves should be destroyed after the profiles are created.

Suspicionless seizures and profiling should be allowed to continue because the seizures themselves invade privacy interests only minimally and because the government's ability to store profiles of DNA taken from members of rationally drawn, statutorily prescribed groups is a valuable law enforcement tool. As many have argued, subjects suffer little as a direct result of biological-sample seizures because DNA-extraction procedures are relatively noninvasive,[191] and because the profile by itself (as opposed to in comparison with other profiles) is basically innocuous.[192] Additionally, suspicionless seizures and profiling allow the government to keep subjects' identifying information on file and ready for use if a subject later becomes a suspect in an investigation. Thus, under such a system, the profiles actually would serve the true-identity function that proponents tout, and the profiles would be available for law enforcement use regardless of the later unavailability of the subject herself.[193] However, to protect subjects' privacy interests in their genetic material and definitively solve one facet of the information-intermingling problem that DNA presents, courts should order the biological samples to be destroyed after the profile is created.[194]

Then, as with post-seizure computer searches, courts should require the government to obtain a search warrant—based on probable cause to believe that the DNA profile to be searched will produce evidence of the crime under investigation—before the government is allowed to search a DNA profile that it created.[195] Requiring a warrant and probable cause would resolve the other facet

191. *See* Wilson v. Collins, 517 F.3d 421, 428 (6th Cir. 2008) ("[T]he swabbing of saliva to obtain a DNA sample is even less invasive than the drawing of a blood sample."); *cf.* Johnson v. Quander, 440 F.3d 489, 496 (D.C. Cir. 2006) (citing Supreme Court precedent approving compelled blood-alcohol tests as a relatively small privacy invasion).

192. *See* Etzioni, *supra* note 95, at 217 ("[P]roponents of DNA databases argue that [genetic profiles] do not provide any meaningful information about individuals aside from allowing [analysts] to determine whether two samples come from the same person.").

193. *See supra* notes 115–118 and accompanying text.

194. In Wisconsin, the current policy is to destroy subjects' biological samples after profiles are created. Suter, *supra* note 5, at 334 & n.172. That is likewise the policy in several European countries that maintain DNA databases. SHELDON KRIMSKY & TANIA SIMONCELLI, GENETIC JUSTICE: DNA DATABANKS, CRIMINAL INVESTIGATIONS, AND CIVIL LIBERTIES 182 (2011).

195. *See* Johnson v. United States, 333 U.S. 10, 14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman . . . .").

of the information-intermingling problem by narrowing the returns on DNA searches to information likely to be relevant to the investigation, thereby minimizing needless privacy invasion and justifying what invasion does occur.[196] Additionally, requiring a judge's determination of probable cause before each search would reaffirm constitutional values by "interpos[ing] a magistrate between the citizen and the police," instead of leaving CODIS subjects vulnerable to zealous officers' determinations of when searching their genetic code is reasonable.[197]

Ironically, in some respects, computer-search procedures even promise a more effective vindication of Fourth Amendment principles in the context of DNA evidence than they currently furnish to computer searches. For instance, commentators such as Josh Goldfoot have criticized as formalistic the requirement that, in conducting a computer search, police must obtain a second warrant in order to pursue evidence of a crime that they discover in the process of their initial warranted search: "Formally, [the second warrant] authorizes the officer to search for new things on the same hard drive. Practically, it simply lets the officer examine evidence that he already has, so that he can read what he has already read."[198] The quandary arises because in searching a computer, officers must open every file, as computers can be configured to misdirect or deceive.[199] Thus, the multiple-warrant requirement provides only formal privacy protections to subjects of computer searches because it does not actually save their personal files from investigators' prying eyes. Rather, its only real consequence is to disallow the state's use of computer evidence of the extrawarranted crime at trial if the investigator failed to obtain a second warrant before searching for the extrawarranted evidence.[200]

Genetic-profile searches are not subject to the same practical constraints. Instead of storing information in scattered and misleading

196. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) ("[A]ny intrusion in the way of search or seizure is an evil, so . . . no intrusion at all is justified without a careful prior determination of necessity." (emphasis omitted)).

197. McDonald v. United States, 335 U.S. 451, 455 (1948).

198. Goldfoot, *supra* note 153, at 144.

199. United States v. Burgess, 576 F.3d 1078, 1095 (10th Cir. 2009); United States v. Giberson, 527 F.3d 882, 889–90 (1st Cir. 2008).

200. Goldfoot, *supra* note 153, at 144–45; *see also* United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1176 (9th Cir. 2010) (per curiam) ("The problem can be stated very simply: There is no way to be sure exactly what an electronic file contains without somehow examining its contents . . . .").

locations, DNA-profile information is tucked tidily away in the government's database, making it easy for police to isolate and search some profiles without disturbing others. As a result, requiring a warrant to search specified profiles in the government's possession would be an extremely effective means of limiting the government's needless exposure of unsuspected subjects' private information, but it would not compromise the effectiveness of the government's search of the relevant subjects' profiles.

CONCLUSION

Thus far, judges have sanctioned legislatures' creation of a multistep DNA-database search process whereby the reasonableness and minimal invasiveness of the first step are permitted to shield later steps' intrusions from constitutional scrutiny. The extraction of blood and the generation of a genetic profile from noncoding sites on the genome may intrude only slightly upon a subject's privacy interests. However, considered in those terms, the government's interest in possessing the blood and profile also is slight. The value of the genetic profile, both to police and to the subject's privacy, exists only when the genetic profile is compared with other profiles because only then can the profile disclose information about biological relationships and physical movements. Therefore, to address the real governmental and privacy interests at stake, the Fourth Amendment discussion of DNA-collection statutes should begin at the point of comparison—not at the point of extraction. This Note has attempted to do just that and has argued that because DNA-database subjects have an actual and reasonable expectation of privacy in their genetic profiles even after their biological samples are in government hands, DNA-database searches are "searches" under the Fourth Amendment.

This Note also has argued that DNA-database searches are unreasonable as they are currently conducted because they lack individualized suspicion and warrant authorization and because they so closely resemble general-warrant computer searches. It has further argued that computer-search procedures suggest a constitutionally preferable alternative because those procedures were developed to guard against the same kind of danger posed by unrestrained DNA-database searches and because they recognize continuing reasonable expectations of privacy following a government seizure. The only question that remains, then, is a normative one: as a society, do we

really believe that a computer is more deserving of privacy protections than our DNA?